Pirates without Borders: the Propagation of Cyberattacks through Firms' Supply Chains

Matteo Crosignani[1] Marco Macchiavelli[2] André F. Silva[2]

[1]New York Fed [2]Federal Reserve Board

2021 Federal Reserve Stress Testing Research Conference

October 8, 2021

The views expressed are solely my own and do not necessarily reflect those of the Board of Governors of the Federal Reserve System or of the Federal Reserve Bank of New York

Motivation

1. **Cyberattacks** are one of the most pressing concerns for firms

WORLD ECONOMIC FORUM

Top ten risks in North America	Top ten risks in Europe
1. Cyberattacks	1. Cyberattacks
2. Data fraud or theft	2. Asset bubble
3. Terrorist attacks	3. Interstate conflict
4. Critical information infrastructure breakdown	4. Energy price shock
5. Failure of critical infrastructure	5. Fiscal crises

- Cyber risk literature focuses on **data breaches**
  - reputation and litigation risk
  - but no systemic consequences, no disruption of productive capacity
- **Ransomware** attacks are different
  - by criminals for financial gain; by state-actors for hybrid warfare
  - can disrupt productive capacity by freezing IT infrastructure

Motivation

2. By disrupting production, cyberattacks can propagate through complex and global **supply chain** networks
   - Customer-supplier relationships are *key for the transmission of shocks* e.g., natural disasters (Barrot and Sauvagnat, 2016); credit supply shocks (Costello, 2020); pandemics (Bonadio et al., 2021)
   - *Unique features of cyberattacks* $\rightarrow$ intentional; spread instantaneously without warning signs; often not geographically clustered

- Increased attention to the impact of data breaches on firms

  $\rightarrow$ but *no empirical evidence* on whether the effects of cyberattacks can be *propagated through customer-supplier relationships* ...

Findings

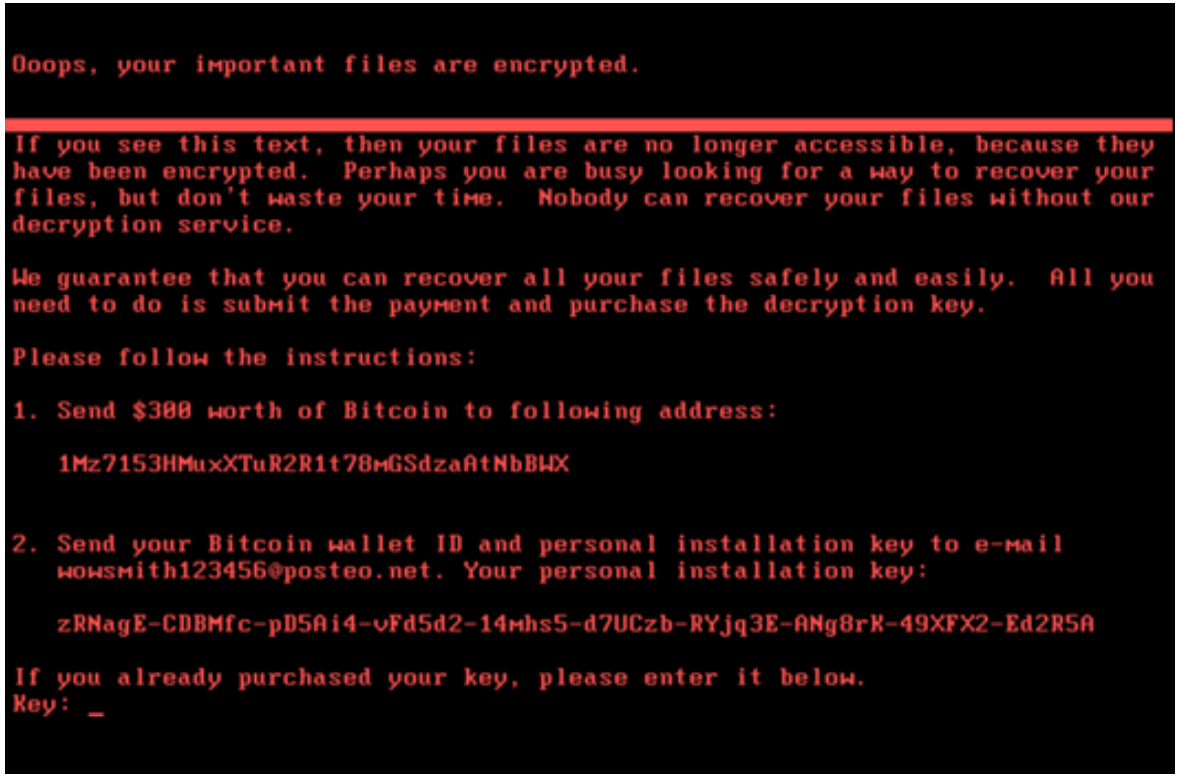
- This Paper: what are the effects of severe cyberattacks on the productive sector?
- Setting: analysis of the **most damaging cyberattack in history** so far that spread inadvertently beyond its target and affected several firms around the world

Preview of Results

1. *Cyberattacks on directly hit firms **propagates downstream** to their customers, amplifying the initial shock four times*
2. *Affected customers deplete **liquidity buffers** and increase borrowing through **bank credit lines**, allowing them to maintain investment and employment*
3. *Affected customers form **new relationships** with alternative suppliers & **terminate the relationship** with the directly hit supplier*

Background

- Unexpected, large-scale **cyberattack in June 2017** ("**NotPetya**")



- Effort by the Russian military intelligence targeted at Ukraine (CIA, 2018)
- Initial vector of infection was a software widely used for tax reporting
  - Appeared to be a ransomware, but true intent was to encrypt and paralyze the computer networks of Ukrainian organizations

Background

- Cyberattack inadvertently spread beyond its original target and **infected global firms** through their Ukrainian subsidiaries ▸ News

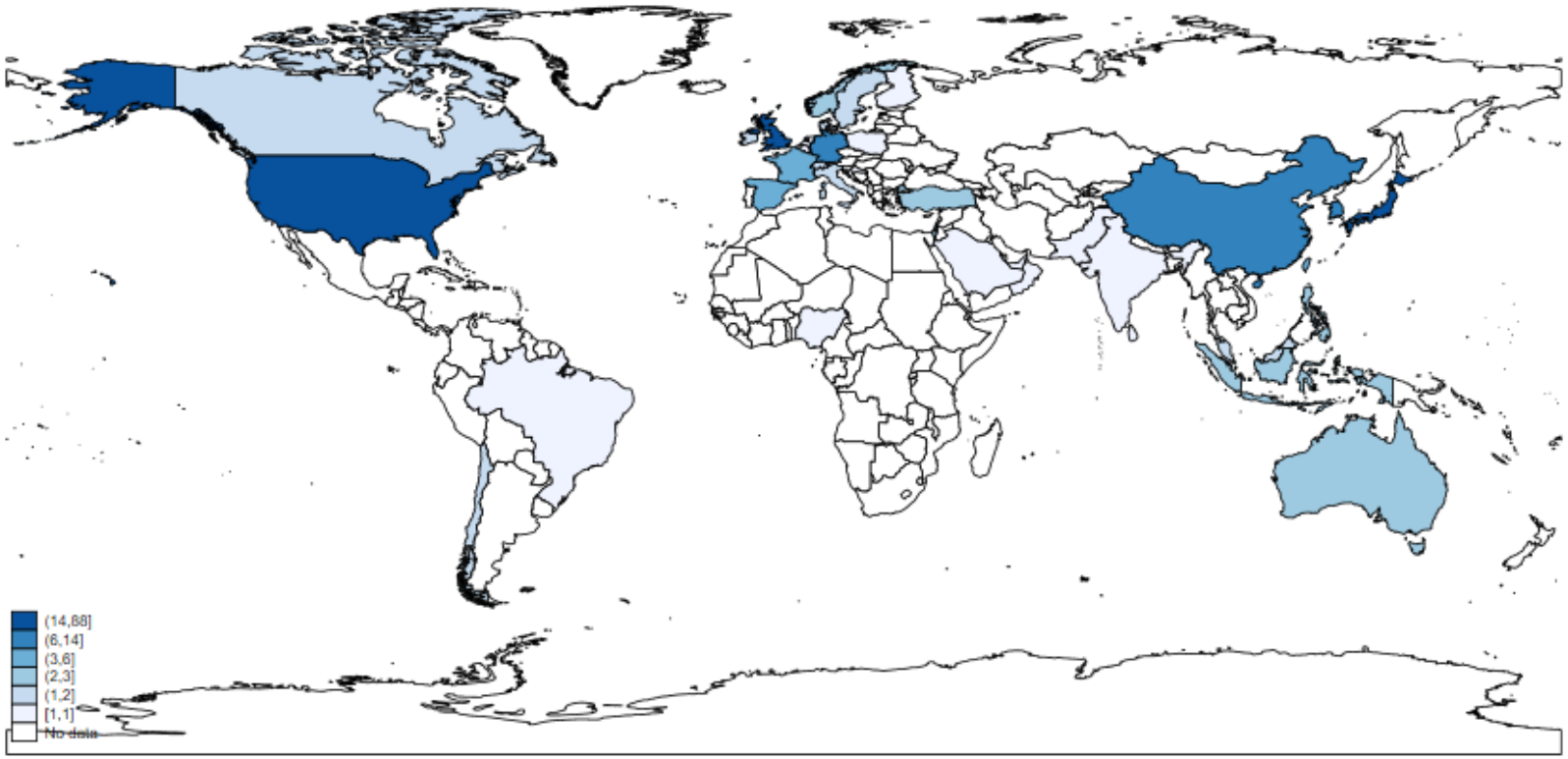
- 8 DIRECTLY HIT FIRMS – large, global, and public (losses: $1.8bn)
  - Merck (US): $670mn
  - FedEx (US): $400mn
  - Maersk (Denmark): $300mn
  - Mondelez (US): $180mn
  - Reckitt Benckiser (UK): $117mn
  - Nuance Communications (US): $92mn
  - Beiersdorf (Germany): $43mn
  - WPP (UK): $15mn

▸ Stock Price Reaction

Background

- Cyberattack inadvertently spread beyond its original target and **infected global firms** through their Ukrainian subsidiaries ▸ News

- 233 INDIRECTLY AFFECTED CUSTOMERS



Data

1. *Directly hit firms:* **SEC filings** and **Dow Jones Factiva**
   - Scraping SEC filings in 2017 and 2018 (keywords: "Petya", "NotPetya", and "Cyber")
   - Manually check over 4,500 newspaper articles worldwide citing NotPetya – available in the Dow Jones Factiva database
   - Cross-check the list of directly hit firms with Greenberg (2019), a book about NotPetya and other cyberattacks

2. *Global supply chain relationships:* **FactSet Revere**
   - Almost 1 million relationships between large (mostly publicly-listed) firms around the world
   - Each customer-supplier relationship has information on the start date, end date, and relationship type

Data

3. *Global firm-level data:* **BvD Orbis** (part of Moody's Analytics)
   - B/S information for more than 350 million firms worldwide
   - Orbis and FactSet merged using ISINs → keep firms present in both data sets
     - 70,590 firm-year observations
     - 15,781 firms; 2014 to 2018
     - 233 affected customers, 320 affected suppliers

4. *Loan-level data for the US:* **Federal Reserve Y-14Q**
   - Information at the quarterly frequency on all credit exposures exceeding $1 million for banks with more than $50 billion in assets
   - Merged with Orbis-FactSet sample using TINs and CUSIPs
     - 137,630 bank-firm-quarter observations
     - 37 banks and 1,997 firms; 2014:Q1 to 2018:Q4
     - 85 affected customers → 87% of US customers in Orbis-FactSet

Identification strategy

- **Difference-in-differences** comparing, before and after the shock:
  1. Firms indirectly affected by cyberattack through their supply chain
  2. Unaffected firms operating in the same industry, country, and size quartile in the same year

Firm-level Analysis

$$Y_{ijt} = \alpha + \beta \text{Post}_t \times \text{Affected}_i + \xi_i + \eta_{jt} + \epsilon_{ijt} \quad (1)$$

- Y_{ijt}: EBIT/assets, long-term debt/assets, liquidity ratio
- $Post_t$: =1 for 2017 and 2018, =0 otherwise
- $Affected_i$: =1 if a firm is a customer/supplier of directly hit firm, =0 otherwise
- ξ_i: firm FE to control for unobserved time-invariant firm characteristics
- η_{jt}: peer group of firm $i \rightarrow$ industry-country-size quartile-year combination
  - *Robustness tests:* industry/country-size quartile-year-linked to affected industry FE

    e.g., for customers: control group firms are not only in the same industry/country and have similar size than the treated customer, but also *use comparable suppliers*

Identification strategy

Loan-level Analysis

$$Y_{ibjt} = \alpha + \beta \text{Post}_t \times \text{Affected}_i + \xi_i + \eta_{jt} + \gamma_{bt} + \epsilon_{ibjt} \quad (2)$$

- Y_{ibjt}: total committed credit, total committed credit lines, share of the committed line of credit that is drawn down, interest rate spread, bank's subjective default probability of the borrower, dummy equal to one if the loan is non-performing, maturity of the committed exposure, amount of collateral
- $Post_t$: =1 after 2017:Q2, =0 otherwise
- $Affected_i$: =1 if a firm is a customer of a directly hit firm, =0 otherwise
- ξ_i: firm FE to control for unobserved time-invariant firm characteristics
- η_{jt}: peer group of firm $i \rightarrow$ industry-state-size quartile-quarter combination
- γ_{bt}: bank-quarter FE to control for time-varying bank characteristics and absorb bank-specific shocks to credit supply

Results

– Part 1 –

Can the effects of cyberattacks on directly hit firms propagate downstream to their customers?

1.1. Downstream Propagation to Customers

	Profitability (EBIT/Assets)				
	(1)	(2)	(3)	(4)	(5)
$\text{Post}_t \times \text{Affected Customer}_i$	-0.010**	-0.012**	-0.013**	-0.015**	-0.012**
	(0.004)	(0.006)	(0.006)	(0.006)	(0.006)
Fixed Effects					
Firm	✓	✓	✓	✓	✓
Industry-Country-Year	✓				
Industry-Size-Year		✓			
Industry-Country-Size-Year			✓		
Country-Size-Linked to Affected Industry-Year				✓	
Industry-Size-Linked to Affected Industry-Year					✓
Observations	66,225	69,827	62,309	45,583	45,886
R-squared	0.757	0.740	0.762	0.745	0.748

- Disruption caused by the cyberattack strongly propagated downstream
  - Economically significant impact: a 1.3 percentage points drop in profitability, corresponding to 25% of the sample median
  - Conservative estimate: $7.3bn loss, a four-fold amplification of the direct impact

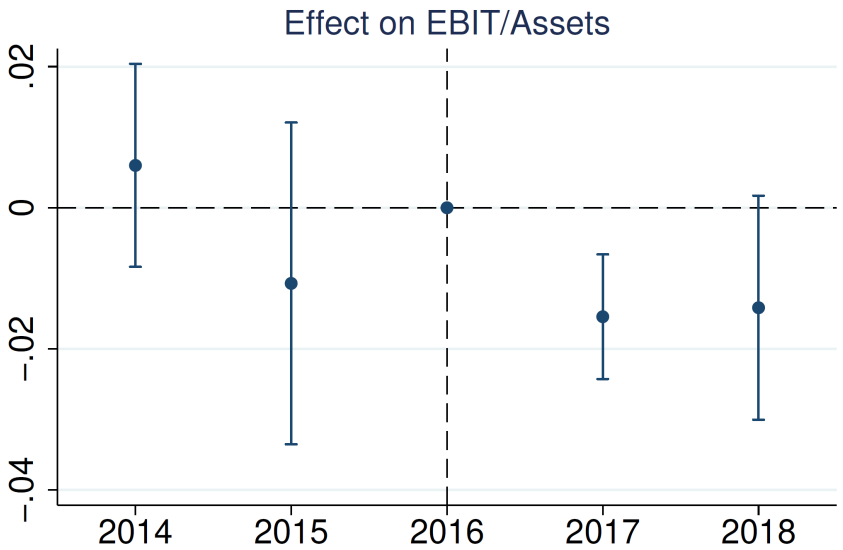
1.2. Supply Chain Vulnerabilities – Alternative Suppliers

	Profitability (EBIT/Assets)				
	(1)	(2)	(3)	(4)	(5)
$\text{Post}_t \times \text{Affected Customer}_i \times$ 1-4 Suppliers_i	-0.022*	-0.023*	-0.029**	-0.024**	-0.024*
	(0.009)	(0.012)	(0.012)	(0.010)	(0.012)
$\text{Post}_t \times \text{Affected Customer}_i \times$ 5+ Suppliers_i	0.001	0.000	0.002	-0.005	0.001
	(0.006)	(0.006)	(0.009)	(0.008)	(0.006)
Fixed Effects					
Firm	✓	✓	✓	✓	✓
Industry-Country-Year	✓				
Industry-Size-Year		✓			
Industry-Country-Size-Year			✓		
Country-Size-Linked to Affected Industry-Year				✓	
Industry-Size-Linked to Affected Industry-Year					✓
Observations	66,225	69,827	62,309	45,583	45,886
R-squared	0.757	0.740	0.762	0.745	0.748

- Supply chain disruption is concentrated on customers with few suppliers in the same industry of the directly hit supplier
- Similar shock amplification for customers of firms selling highly specific inputs

▸ Table

1.3. Additional Propagation Results



- Parallel trends assumption holds → firm characteristics are also similar across treatment and control group within size quartiles
- No further downstream effect (customers of customers)
- No upstream propagation effect on suppliers of directly hit firms
  - Shock impaired the directly hit firms' ability to deliver products to their customers, but not the suppliers' ability to deliver products to directly hit firms

Results

– Part 2 –

How do the firms in the supply chain cope with the shock? Do banks play a role in mitigating its impact?

2.1. Cyberattack and Liquidity Risk Management

	Liquidity Ratio (current assets-inventories/current liabilities)				
	(1)	(2)	(3)	(4)	(5)
$\text{Post}_t \times \text{Affected Customer}_i$	-0.156***	-0.201***	-0.291***	-0.255***	-0.225***
	(0.030)	(0.073)	(0.044)	(0.036)	(0.055)
Fixed Effects					
Firm	✓	✓	✓	✓	✓
Industry-Country-Year	✓				
Industry-Size-Year		✓			
Industry-Country-Size-Year			✓		
Country-Size-Linked to Affected Ind-Year				✓	
Industry-Size-Linked to Affected Ind-Year					✓
Observations	66,225	69,827	62,309	45,583	45,886
R-squared	0.759	0.741	0.764	0.754	0.753

- To deal with the shock, affected customers relied on their internal liquidity
- They also increase external borrowing...

2.2. Role of Banks – Loan-level Evidence from the US

	Log(Tot Committed)		Log(Committed Line)		Sh Drawn Credit	
	(1)	(2)	(3)	(4)	(5)	(6)
$\text{Post}_t \times \text{Affected}_i$	-0.037	-0.199	-0.018	0.097	0.045**	0.084**
	(0.091)	(0.165)	(0.051)	(0.060)	(0.020)	(0.038)
Fixed Effects						
Firm	✓	✓	✓	✓	✓	✓
Bank-Quarter	✓	✓	✓	✓	✓	✓
Ind-State-Quarter	✓		✓		✓	
Ind-State-Size-Quarter		✓		✓		✓
Observations	137,630	131,428	129,756	123,936	129,756	123,936
R-squared	0.581	0.583	0.624	0.623	0.586	0.620

- Affected customers significantly increase credit line draw downs to cope with the pressing liquidity needs $\rightarrow$ highlights the liquidity insurance function of banks

2.2. Role of Banks – Loan-level Evidence from the US

	Rate Spread	Pr(Default)	NPL	Maturity	Collateral
	(1)	(2)	(3)	(4)	(5)
$\text{Post}_t \times \text{Affected}_i$	0.146***	1.559**	0.002	-0.279	0.028
	(0.021)	(0.669)	(0.015)	(2.713)	(0.288)
Fixed Effects					
Firm	✓	✓	✓	✓	✓
Bank-Quarter	✓	✓	✓	✓	✓
Ind-State-Size-Quarter	✓	✓	✓	✓	✓
Observations	131,428	104,591	131,428	130,890	114,641
R-squared	0.608	0.547	0.055	0.595	0.498

- Increase in perceived riskiness of affected customers
  - No bias arising from affected customers matching with banks offering less competitive pricing $\rightarrow$ results are within bank-quarter, comparing the rate charged by the same bank to affected and unaffected firms
- Consistent with affected customers able to raise liquidity, we do not find effects on employment and investment

Results

– Part 3 –

Do customer-supplier networks change in response to cyberattacks?

3. Disruptions and Supply Chain Adjustments

1. Affected customers more likely to form **new trading relations** $\rightarrow$ within the 1^{st} **year** after the shock and among those with vulnerable supply chains: wake-up call

2. Affected customers more likely to **terminate the trading relation** with directly hit supplier $\rightarrow$ only in the 2^{nd} **year** after the shock: reputation effect

▶ Tables

Conclusion

- We examine the **economic impact** and **supply chain effects** of the **most damaging cyberattack in history** so far

1. Downstream propagation effects $\rightarrow$ considerable reduction in profits among customers of directly hit firms
2. Affected customers depleted pre-existing liquidity buffers and increased borrowing through bank credit lines, which allowed them to maintain investment and employment
3. There are persisting adjustments to the supply chain network following the shock

- POLICY IMPLICATIONS: given how interconnected firms are at a global scale, results highlight the need to have better cybersecurity and contingency planning, as well as a more diversified supply chain

FINANCIAL TIMES

Maersk, WPP and FedEx still struggling with cyber attack fallout

Global companies ranging from shipping lines to advertising firms are still struggling with the havoc wreaked by the huge cyber attack that last week swept from Ukraine to organisations in more than 60 countries.

AP Moller-Maersk, WPP, Reckitt Benckiser and FedEx all said their businesses were still not back to normal after the ransomware attack last week compromised hundreds of thousands of computers, industrial equipment and other technology.

Some ports remain hobbled, packages are going missing and customers are struggling to place and track orders, the companies said.

The New York Times

Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong.

Mondelez was deemed collateral damage in a cyberwar.

When the United States government assigned responsibility for NotPetya to Russia in 2018, insurers were provided with a justification for refusing to cover the damage. Just as they wouldn't be liable if a bomb blew up a corporate building during an armed conflict, they claim not to be responsible when a state-backed hack strikes a computer network.

DW Made for minds.

US charges 6 Russian military intelligence officers over cyberattacks

The hackers attacked the 2017 French elections, the 2018 Winter Olympics, the Ukraine's power grid and investigations into a Novichok poisoning, claims the US. They may also have used the destructive NotPetya malware.

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

WIRED

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

Back

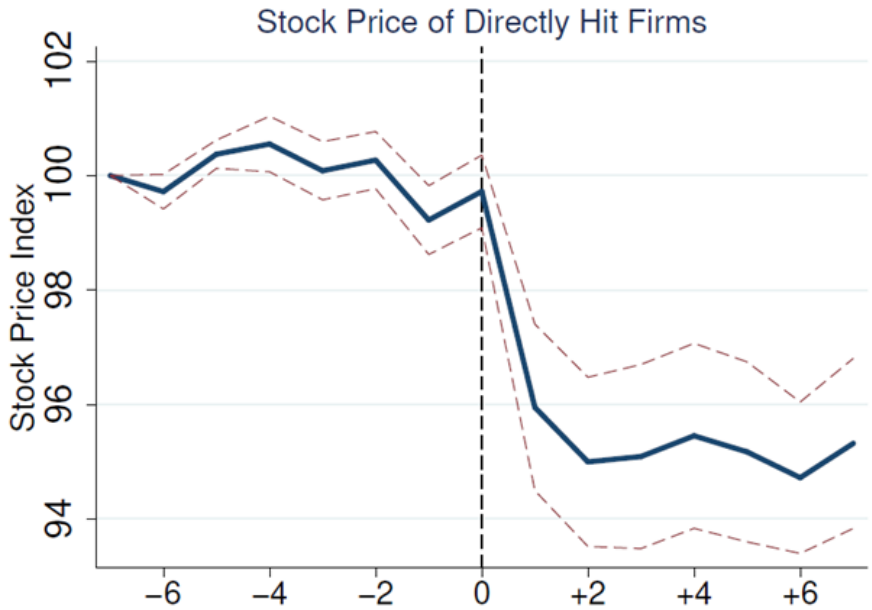


Figure : Stock Price of Directly Hit Firms Around News of the Damages of NotPetya. This figure shows the stock price evolution around the news of the damages of NotPetya (from seven trading days prior to the news to seven days after the news). Stock prices are averaged across firms and normalized to 100 seven trading days before the disclosure of the news. The dashed lines indicate the standard errors around the mean. The dates when the news of the damages were publicly released are as follows: August 16, 2017 for Moller-Maersk (link); August 2, 2017 for Beiersdorf (link); June 28, 2017 for Mondelez (link); August 22, 2017 for WPP (link); June 28, 2017 for Nuance (link); July 16, 2017 for FedEx (link); July 5, 2017 for Reckitt Benckiser (link); October 26, 2017 for Merck (link). Source: Datastream.

Back

1.3. Supply Chain Vulnerabilities – Input Specificity

	Profitability (EBIT/Assets)				
	(1)	(2)	(3)	(4)	(5)
$\text{Post}_t \times \text{Affected Customer}_i \times \text{Specific Input}_i$	-0.011***	-0.015***	-0.017**	-0.019***	-0.016***
	(0.004)	(0.005)	(0.006)	(0.006)	(0.005)
$\text{Post}_t \times \text{Affected Customer}_i \times \text{Not Specific Input}_i$	-0.006	-0.004	-0.004	-0.005	-0.005
	(0.006)	(0.009)	(0.008)	(0.008)	(0.009)
Fixed Effects					
Firm	✓	✓	✓	✓	✓
Industry-Country-Year	✓				
Industry-Size-Year		✓			
Industry-Country-Size-Year			✓		
Country-Size-Linked to Affected Industry-Year				✓	
Industry-Size-Linked to Affected Industry-Year					✓
Observations	66,225	69,827	62,309	45,583	45,886
R-squared	0.757	0.740	0.762	0.745	0.748

- Disruptions among customers more severe when directly affected firm (the supplier) produces a more specific, less substitutable product
  - Supplier producing a highly specific input if it has an above the median ratio of R&D expenditure to sales (Barrot and Sauvagnat, 2016)

Back

3. Disruptions and Supply Chain Adjustments

	New Relations		
	(1)	(2)	(3)
$\text{Post}_{2017} \times \text{Affected Customer}_i$	0.150**	0.128**	
	(0.064)	(0.057)	
$\text{Post}_{2018} \times \text{Affected Customer}_i$	0.001	-0.047*	
	(0.023)	(0.025)	
$\text{Post}_{2017} \times \text{Affected Customer}_i \times \text{1-4 Suppliers}_i$			0.195**
			(0.086)
$\text{Post}_{2017} \times \text{Affected Customer}_i \times \text{5+ Suppliers}_i$			0.056
			(0.068)
$\text{Post}_{2018} \times \text{Affected Customer}_i \times \text{1-4 Suppliers}_i$			-0.061*
			(0.035)
$\text{Post}_{2018} \times \text{Affected Customer}_i \times \text{5+ Suppliers}_i$			-0.031
			(0.047)
Fixed Effects			
Firm	✓	✓	✓
Country-Size Bucket-Linked to Affected Industry-Year	✓		
Industry-Size Bucket-Linked to Affected Industry-Year		✓	✓
Observations	45,583	45,886	45,886
R-squared	0.695	0.696	0.696

- Affected customers more likely to form new trading relations → within the 1st year after the shock and among those with vulnerable supply chains: wake-up call

Back

3. Disruptions and Supply Chain Adjustments

	Ended Relations			Ended Relations excl. Hit Supplier		
	(1)	(2)	(3)	(4)	(5)	(6)
$Post_{2017} \times$ Affected Customer$_i$	0.051	0.024		0.035	0.016	
	(0.043)	(0.044)		(0.049)	(0.048)	
$Post_{2018} \times$ Affected Customer$_i$	0.199***	0.145**		0.067	0.016	
	(0.065)	(0.070)		(0.075)	(0.071)	
$Post_{2017} \times$ Affected C$_i \times$ 1-4 Suppliers$_i$			-0.041			-0.057
			(0.053)			(0.041)
$Post_{2017} \times$ Affected C$_i \times$ 5+ Suppliers$_i$			0.095			0.094
			(0.103)			(0.107)
$Post_{2018} \times$ Affected C$_i \times$ 1-4 Suppliers$_i$			0.127**			-0.040
			(0.049)			(0.027)
$Post_{2018} \times$ Affected C$_i \times$ 5+ Suppliers$_i$			0.164			0.078
			(0.144)			(0.143)
Fixed Effects						
Firm	✓	✓	✓	✓	✓	✓
Country-Size-Linked to Affected Ind-Year	✓			✓		
Industry-Size-Linked to Affected Ind-Year		✓	✓		✓	✓
Observations	45,583	45,886	45,886	45,583	45,886	45,886
R-squared	0.667	0.671	0.671	0.664	0.668	0.669

- Affected customers more likely to terminate the trading relationship with directly hit supplier → only in the 2nd year after the shock: reputation effect

Back